

IN THE UNITED STATES DISTRICT COURT  
FOR THE COMMONWEALTH OF NORTHERN MARIANA ISLANDS

IN THE MATTER OF THE SEARCH OF:  
Unit 14 at Palms Garden Apartments,  
Chinatown, Saipan.

Case No. **MC 21-00001**

**AFFIDAVIT IN SUPPORT OF AN**  
**APPLICATION UNDER RULE 41 FOR A**  
**WARRANT TO SEARCH AND SEIZE**

I, Richard J. Bauer, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search Unit 14 (hereinafter "PREMISES") of the Palms Garden Apartments, as further described in Attachment A, for items described in Attachment B.
2. I am a Special Agent with the Federal Bureau of Investigation and have been for more than six (6) years. I am currently assigned to the FBI Honolulu Field Office, Saipan Resident Agency, where my duties include, but are not limited to, investigating sex & labor trafficking, online production and distribution of child pornography, and other crimes of violence. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and empowered by the law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code. Through my training and experience, I have become familiar with the manner in which criminal offenders operate, and the efforts of those individuals in such activities.
3. During my tenure as a Special Agent with the FBI, I have participated in numerous investigations where I have (a) conducted physical and wire surveillance; (b) executed search

warrants for electronic devices; (c) served as a monitor in federal wiretap cases and overheard conversations of drug traffickers to identify subjects and gather evidence and (d) conducted surveillance of individuals engaged in the sexual exploitation of children, drug traffickers, and other violations of federal and state law.

4. The statements in this affidavit are based in part on information provided by Task Force Officers, other Special Agents of the FBI and on my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Section 2252(a)(4)(B) (possession of child pornography), are presently located at the subject PREMISES.

#### **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

5. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The

distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

6. The development of computers has changed this; computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

7. Child pornographers can now transfer photographs from a camera onto a computer readable format with a device known as a scanner. With the advent of digital cameras, the images can be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through use of a telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

8. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The storage capability of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously over the years. These drives can store hundreds of thousands of images at a very high resolution.

9. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

10. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Microsoft, and Google, among others. The online services allow a user to set up an account with a remote computing service that provides e mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any

computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

11. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer contains peer to peer software, when the computer was sharing files, and even some of the files which were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data.

12. A popular tool used by individuals involved in the collection and distribution of child pornography on the Internet, is peer to peer file sharing (hereinafter, "P2P"). P2P file sharing is a method of communication available to Internet users through use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. P2P software is readily available for download on the Internet and is often available for free. In general, P2P software allows the user to set-up file(s) on his computer so that the files can be shared with others running compatible P2P software. In essence, a user allows his computer to be searched and accessed by other users

of the network. If another user finds a file of interest on his computer, the P2P software allows that other user to download the file from your computer. A user obtains files by opening the P2P software on his computer and typing in a search term or terms. The P2P software then conducts a search of all computers connected to that network to determine whether any files matching the search term are currently being shared by any other user on that network. The P2P software programs known as eMule, Ares Galaxy, LimeWire, FrostWire, and many other types of P2P software, sets up its searches by keywords. The results of a keyword search are displayed to the user. The user then selects file(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and one or more computers on the same network containing the file.

13. The strength of the P2P Networks is that they base all of their file shares on a hashing algorithm. Hashing uses mathematical algorithms which allows for the creation of an alphanumeric value specific and unique to that file, which is the equivalent of a digital fingerprinting of the file. For example, once you check a file with a Secure Hash Algorithm (SHA-1) hashing utility capable of generating this SHA-1 value (the digital fingerprint), that will be a fixed-length unique identifier for that file. The SHA-1 is called secure because it is computationally infeasible for two files with different content to have the same SHA-1 hash value. Law Enforcement can search the P2P networks to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. When a user on the P2P network offers a file to trade, the P2P software used by law enforcement calculates a "hash value" of the file using

a SHA-1 hash. A person may copy a file and rename it but if it is an exact copy, regardless of the name of the file, it will have the same hash value.

14. Most P2P programs allow users to designate specific folder(s) as "shared" folders. Any files contained in those specific folders are then made available for download by other users on the same P2P network. P2P software users typically do not "share" all of the files on their hard drive.

15. The BitTorrent network is a very popular and publicly available P2P file-sharing network. Most computers that are part of this network are referred to as "peers" or "clients," hereafter referred to as a peer. A peer can download files from other peers and simultaneously provide these files to other peers.

16. The BitTorrent network can be accessed by computers via many different client (software) programs, such as the "BitTorrent" program, the "µTorrent" program, the "BitLord" program, and the "Vuze" program, to name a few. These client programs are publicly available, typically free, and can be downloaded from the Internet.

17. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between an investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes 1) the suspect client's IP address; 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) are being reported as shared from the suspect client program; and 3) the BitTorrent network client

program and version being utilized by the suspect computer. Law enforcement has the ability to log this information.

18. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address is unique to a particular computer during a specific online session. The IP address provides a unique "location," or address, as to each computer, making it possible for data to be transferred between computers.

19. The computer running P2P software has an IP address assigned to it while it is connected to the Internet. Investigators are able to see the IP address of any computer system sharing files. Investigators can then search public records that are available on the Internet to determine the specific Internet Service Provider (ISP) who has assigned that IP address to that computer. ISPs maintain logs and records which reflect the specific IP addresses it assigned to specific computers that connect to the Internet through that ISP at any given moment. Based upon the IP address assigned to the computer sharing files, subscriber information then can be obtained from the ISP which contains identifying information of the individual to whom the account is registered.

20. The computers that are linked together to form the P2P network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce. A person who includes child pornography files in his/her "shared" folder is hosting child pornography and therefore is promoting, presenting, and potentially distributing child pornography. A person who hosts child pornography is in violation of Title 18, United States Code, Section 2252A(a)(3)(B)



in that he/she is promoting and presenting child pornography in interstate and foreign commerce by means of a computer.

**SPECIFIC PROBABLE CAUSE**

21. Between July 01, 2020 and July 21, 2020, an FBI Honolulu Child Exploitation Special Agent (SA) conducted an undercover investigative session on the BitTorrent network. The operation targeted individuals sharing child pornography. The investigation discovered that two devices connected to IP addresses 202.123.150.86 and 202.123.150.84, had accessed files that appeared to be related to the distribution of child pornography. The two devices are hereinafter referred to as "Suspect Devices."

22. The SA made a record of suspected child pornography files available on the Suspect Devices that were accessed via IP addresses 202.123.150.86 and 202.123.150.84. As of November 9, 2020, the SA identified 388 files of interest, 241 of which are categorized as severe files by the National Center for Missing and Exploited Children (NCMEC). Descriptions of three of the video files made available by the Suspect Devices are described as follows:

a. File name: *(Pthc) 6YoBaby's – Bedtime rape.mpg*

File size: 11.0 MB

File Description: The length of the video is 1 minute, 3 seconds (00:01:01). The video depicts an adult male performing oral sex on a nude prepubescent female child lying in bed. The adult male then digitally penetrates, and ultimately inserts his penis into the child's vagina and ejaculates.



- b. File name: *4yo Girl And 8Yo Suck Look Ptsc Kleuterkutje Hussyfan Yamad Kingpass Moscow Pedo.mpg*

File size: 144 MB

File Description: The length of the video is 4 minutes and 23 seconds (00:04:23).

The video shows two prepubescent female children performing oral sex on an adult male. The adult male then rubs his penis on one of the female child's vagina. The adult male then ejaculates into one of the female child's mouth.

- c. File name: *3+4yr Girls children sexually abused BEAUTIFUL\_Venezuela part-2).mpg*

File size: 24.5 MB

File Description: The length of the video is 4 minutes and 39 seconds (00:04:39).

The video shows two naked prepubescent female toddlers in a bath. An adult male has his erect penis showing and begins to masturbate. The adult male then has the toddler females perform manual masturbation on him.

23. Pursuant to an administrative subpoena, on July 27, 2020, IT&E, the internet service provider (ISP) for IP Addresses 202.123.150.86 and 202.123.150.84, revealed that the subscriber was R.L. and the GPS coordinates for the addresses were Latitude 15.127138 and Longitude 145.702284.

24. On September 9, 2020, Special Agent Richard J. Bauer, hereinafter your Affiant, conducted surveillance at a compound found at Latitude 15.127138 and Longitude 145.702284. On November 3, 2020, your Affiant attempted to contact the registered owner of the IP Addresses. While at the compound, the landlord, who lived two doors from R.L., advised that she had rented an apartment to R.L., but that R.L. had recently moved to the Palms Garden Apartments in Chinatown, Saipan.

25. Your Affiant interviewed R.L. on November 06, 2020 and learned that she, her husband, and their three school-age daughters moved with all their possessions from their previous apartment during the final week of October 2020 and have stayed at the new location ever since. Prior to the move, however, R.L. explained that her previous internet account was shared between two households, R.L.'s own household and that of her sister, E.S., who lived in the adjacent unit since about 2007. The account was password protected and therefore, during the relevant time period, was accessible only to those two households.

26. R.L. further advised that her household's only electronic devices capable of wireless internet access are three cellular telephones, a smart television, and a laptop used by her oldest, high school-age daughter. Of these devices, only the laptop computer would likely have the necessary capacity and available storage for the files of interest. Based on my knowledge, training, and experience, I know that it is very rare for teenage females to consume child pornography. Therefore it is unlikely that the Suspect Devices will be found at R.L.'s new residence.

27. Meanwhile, the investigation revealed that E.S. lived with her common-law husband and adult-age son at the time the files cited in paragraph 22 were accessed. Based on my knowledge, training, and experience, I know that adult-age males are, by far, the largest consumers of child pornography. *See e.g., Child Molesters: A Behavioral Analysis*, Kenneth V. Lanning (5<sup>th</sup> Ed. 2010) at p. 121, *citing National-Juvenile Online Victimization Study*, Wolak, Mitchell, and Finklehorn, 2003). Accordingly, there is a reasonable probability that the Suspect Devices will belong to either the common-law husband or adult-age son.

28. Based on this information, on December 18, 2020, your Affiant obtained a warrant to search E.S.'s unit at the compound located at Latitude 15.127138 and Longitude 145.702284. A team of federal agents sought to execute the search warrant on December 21, 2020, but upon arrival at the location, learned from the landlord that within the last two weeks, E.S. had moved with her family and its possession to the same apartment building as her sister, R.L.

29. The team did not execute the search warrant, but was able to confirm through the new tenants and the landlord that neither ~~R.L.~~ <sup>E.S. (250)</sup>, nor her common law husband, nor her adult age son had left behind any computers or similar electronic devices, and therefore, most likely brought them to the new domicile.

30. In the morning of January 6, 2021, just prior to the execution of this warrant, FBI Special Agent Haejun Park interviewed E.S. at the PREMISES, specifically, Unit 14 at the Palms Garden Hotel. E.S. confirmed that she lived with her 53-year old, common law husband, and her 23-year old male son, and recently moved into the PREMISES with all of their possessions, to include one laptop computer capable of accessing the internet, from their previous residence.

E.S. confirmed that at her previous residence, her household shared IT&E internet services with her sister, R.L., and the account was password protected, so only residents of the two households could have accessed the internet using the particular IP addresses assigned to her. E.S. also advised that there was one computer in the PREMISES which was used exclusively by her son.

### **TECHNICAL TERMS**

31. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

### **CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS**

32. Most individuals who collect child pornography are sexually attracted to children, their sexual arousal patterns and erotic imagery focus, in part or in whole, on children. The collection may be exclusively dedicated to children of a particular age/gender or it may be more diverse, representing a variety of sexual preferences, including children. Child pornography collectors

express their attraction to children through the collection of sexually explicit materials involving children as well as other seemingly innocuous material related to children.

33. These individuals may derive sexual gratification from actual physical contact with children as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children.

34. Visual depictions may range from fully clothed depictions of children engaged in non-sexual activity to nude or partially nude depictions of children engaged in explicit sexual activity. In addition to child pornography, these individuals are also highly likely to collect other paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica" which is defined as any material, relating to children, that serves a sexual purpose for a given individual. It is broader and more encompassing, than child pornography, but at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his intent. It includes things such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons and non-sexually explicit visual images.

35. Child pornography collectors reinforce their fantasies, often by taking progressive, overt steps aimed at turning the fantasy into reality in some or all of the following ways: collecting and organizing their child-related material; masturbating while viewing the child pornography;

engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need-driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.

36. Child pornography collectors almost always maintain and possess their material in the privacy and security of their homes or some other secure location where it is readily available. The collection may include sexually explicit or suggestive materials involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images or other visual media. The collector is aroused while viewing the collection and, acting on that arousal, he often masturbates, thereby fueling and reinforcing his attraction to children. This is most easily accomplished in the privacy of his own home.

37. Because the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished sexual fantasies, the collector may not dispose of the collection. The collection may be culled and refined over time, but the size of the collection tends to increase. Individuals who use a collection in the seduction of children or to document that seduction treat the materials as prized possessions and are especially unlikely to part with

them. Even if a child pornography collector does delete files from his hard drive or other electronic media, a computer expert can still retrieve those files using forensic tools.

**COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

38. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

39. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few



examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

40. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether

data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to obtain child pornography over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

41. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

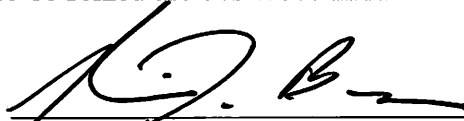
42. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

43. It is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined

that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

**CONCLUSION**

44. I submit that this affidavit supports probable cause for a warrant to search the property described in Attachment A and the items to be seized are described in Attachment B.



Richard J. Bauer  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me  
on January 6, 2021:



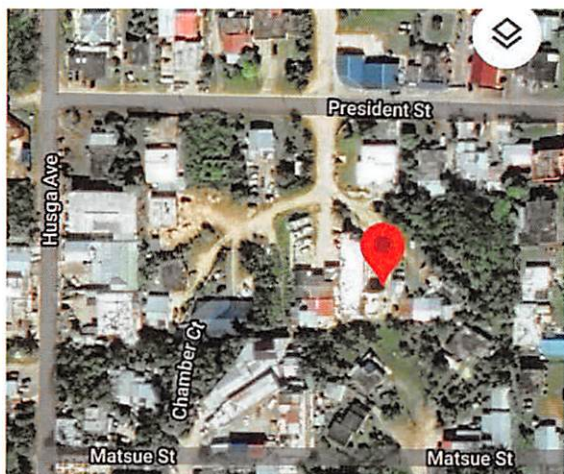
THE HONORABLE RAMONA V. MANGLONA  
UNITED STATES CHIEF JUDGE



ATTACHMENT A

*Property to be searched*

The property to be searched is located off President St., as indicated by the red balloon on the map below:



It is a two-story apartment complex at the with approximately 10 units on each level, and is marked “Palms Garden Apartments” on the north side of the building, as seen in this photograph:



Unit 14 is a ground level apartment with a light beige colored door clearly marked with a “14” at the entry way.

**ATTACHMENT B**

*Property to be seized*

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 2252 (a)(4)(B):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
  - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
  - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;



- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
  - h. evidence of the times the COMPUTER was used;
  - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
  - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - k. records of or information about Internet Protocol addresses used by the COMPUTER;
  - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
  - m. contextual information necessary to understand the evidence described in this attachment.
3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography and child erotica.
5. Records, information, and items relating to violations of the statutes described above including
- a. Records, information, and items relating to the occupancy or ownership of PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
  - b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media

that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.